Biztonság és védelem az informatikában

2. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

Felhasznált programok:

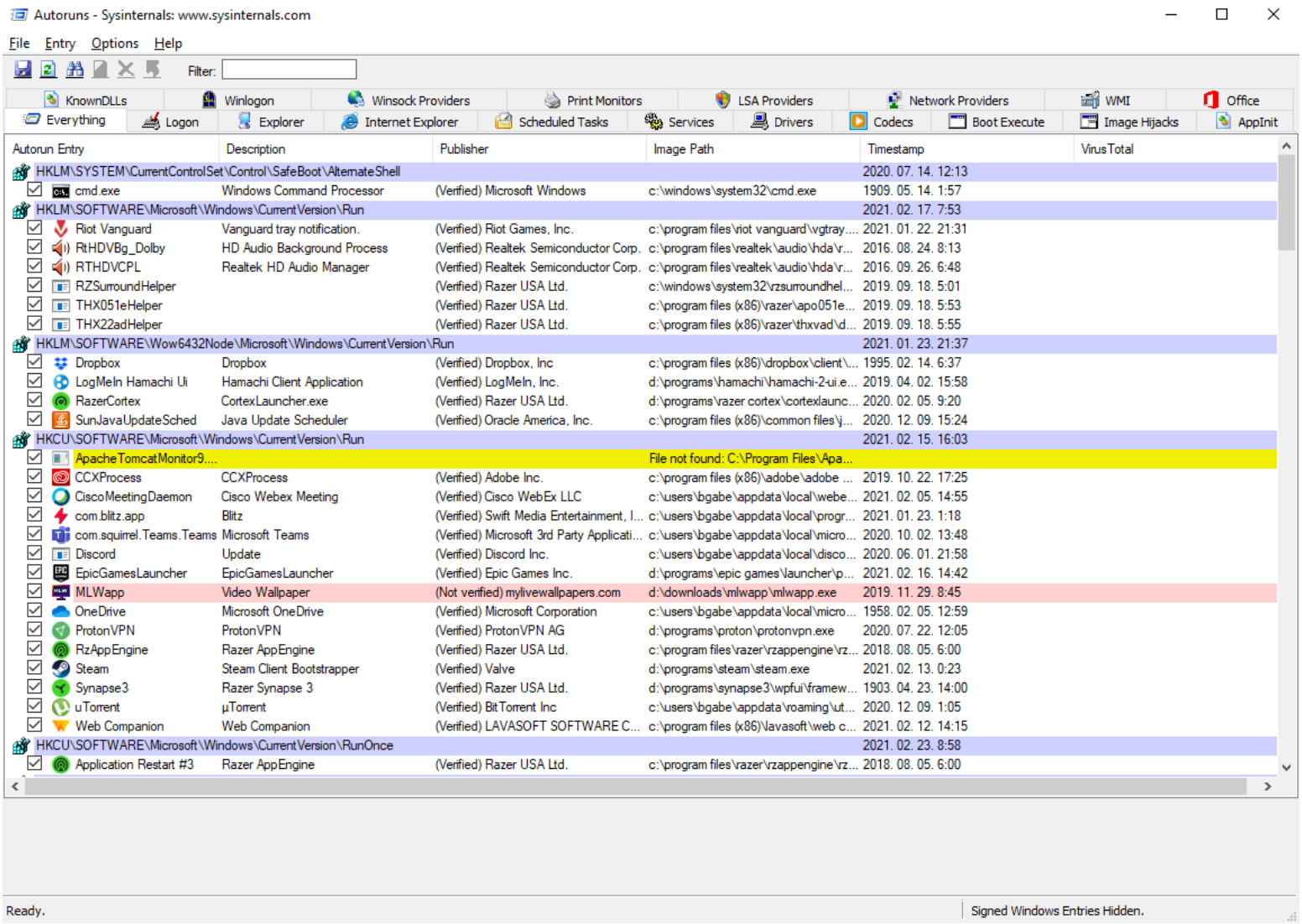
WindowsPortableApps, TcpView, ProcessExplorer, AutoRuns, WireShark

2021.02.18

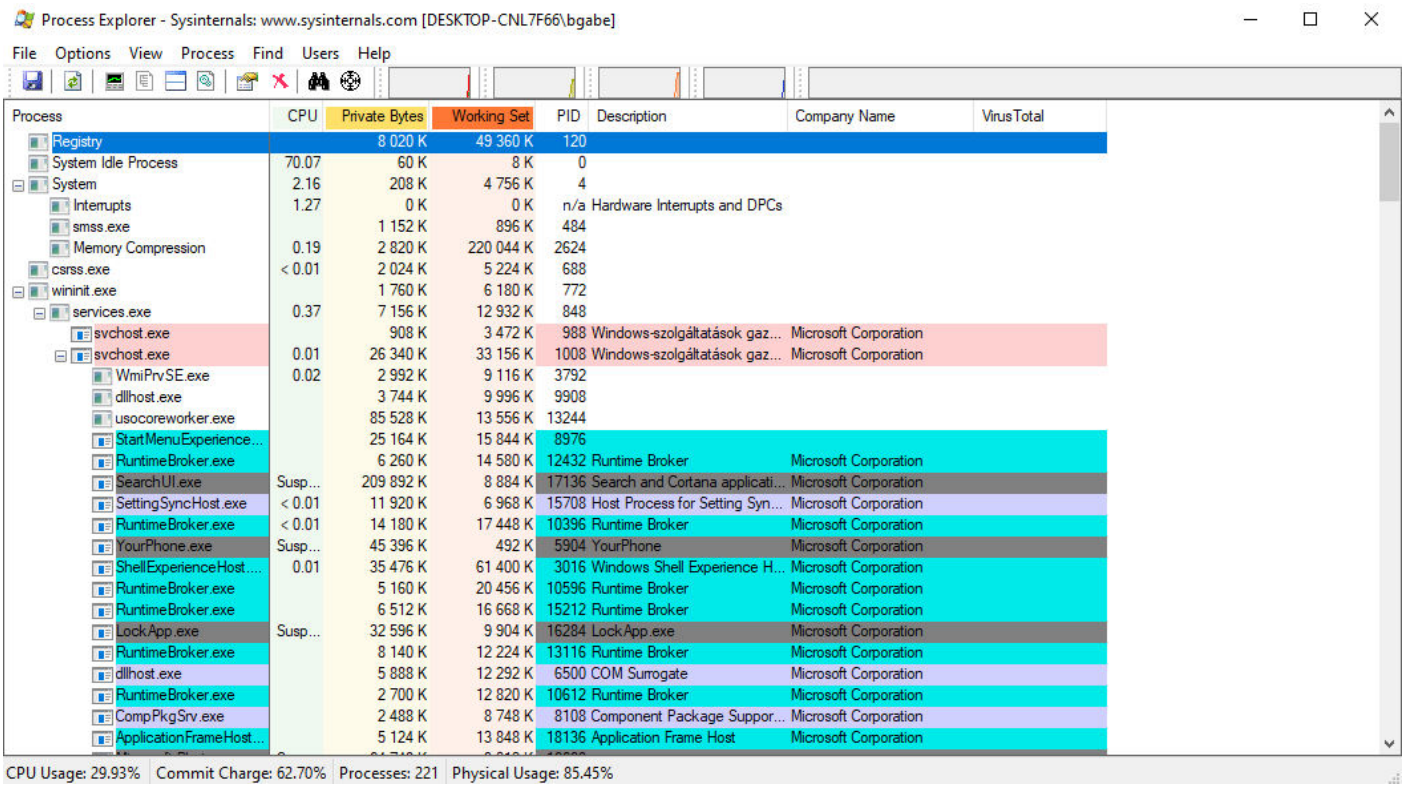
Bot, Worm behatoló detektálása

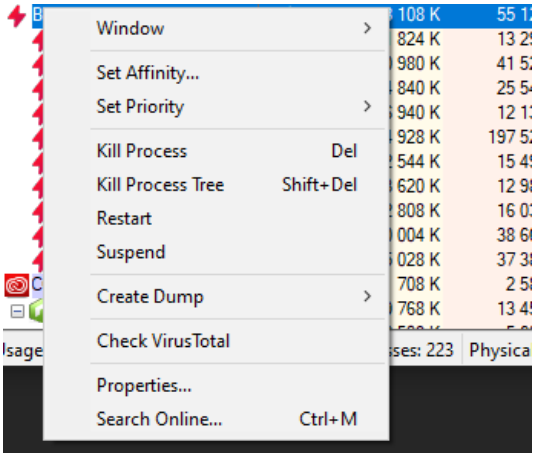
Miután a leírtak szerint letöltöttem a WindowsPortableApps, tcpView, ProcessExplorer és AutoRuns alkalmazásokat, és a licenseket is jóváhagytam az Autoruns programot indítottam el.

Ezen alkalmazás segítségével a jelenleg futó alkalmazásokat tudom megtekinteni:



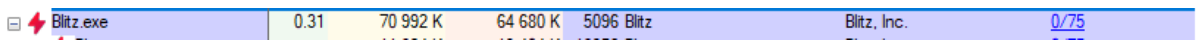
A részletesebb vizsgálathoz ProcessExplorer-t használtam, melyet a feladat leírásban megjelölt linken töltöttem le.

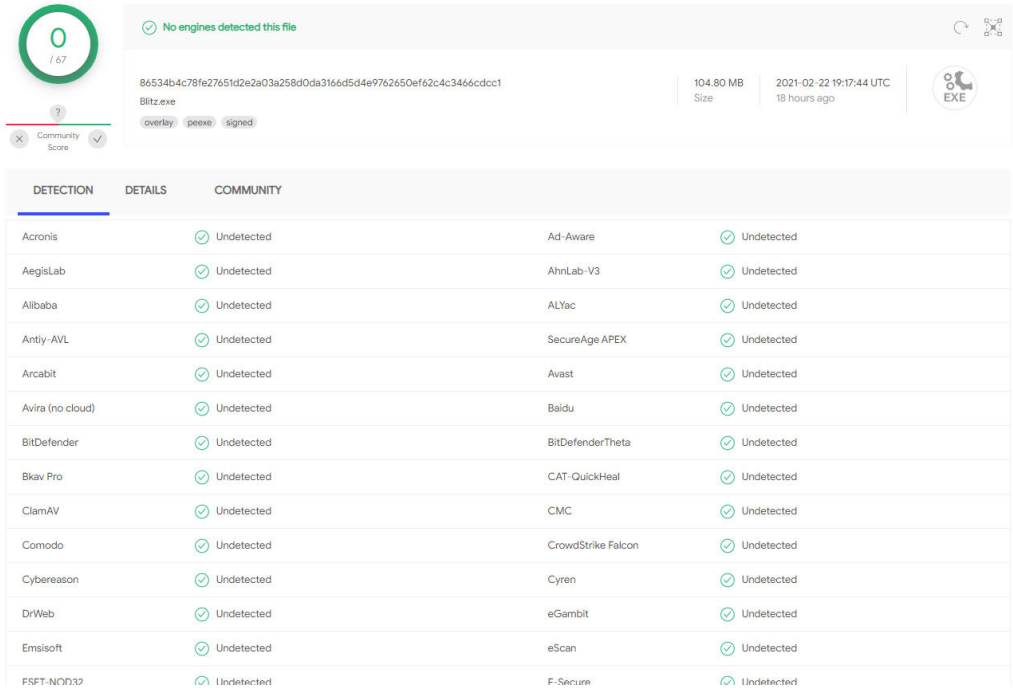




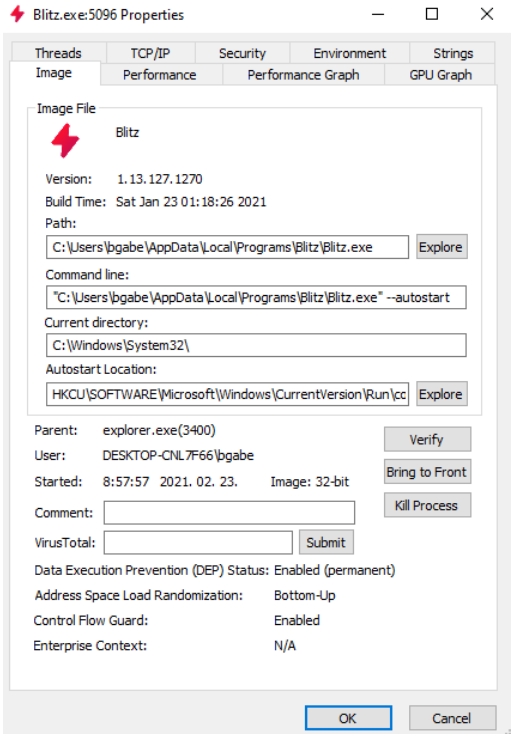
Lehetőségünk van leállítani újraindítani elindítani, illetve felfüggeszteni az alkalmazásokat.

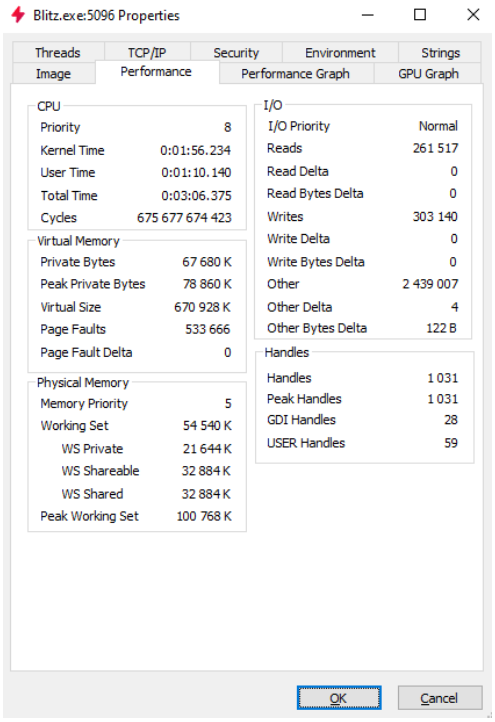
Gyanús programok esetén még esélyünk van egy Check VirusTotal lehetőségre is mely során a programról készített egyedi hash-t vírus keresőket tartalmazó weblapra küldi el, majd megtekinthetjük az eredményeket a legutolsó sorban lévő '0/75'- re kattintva.



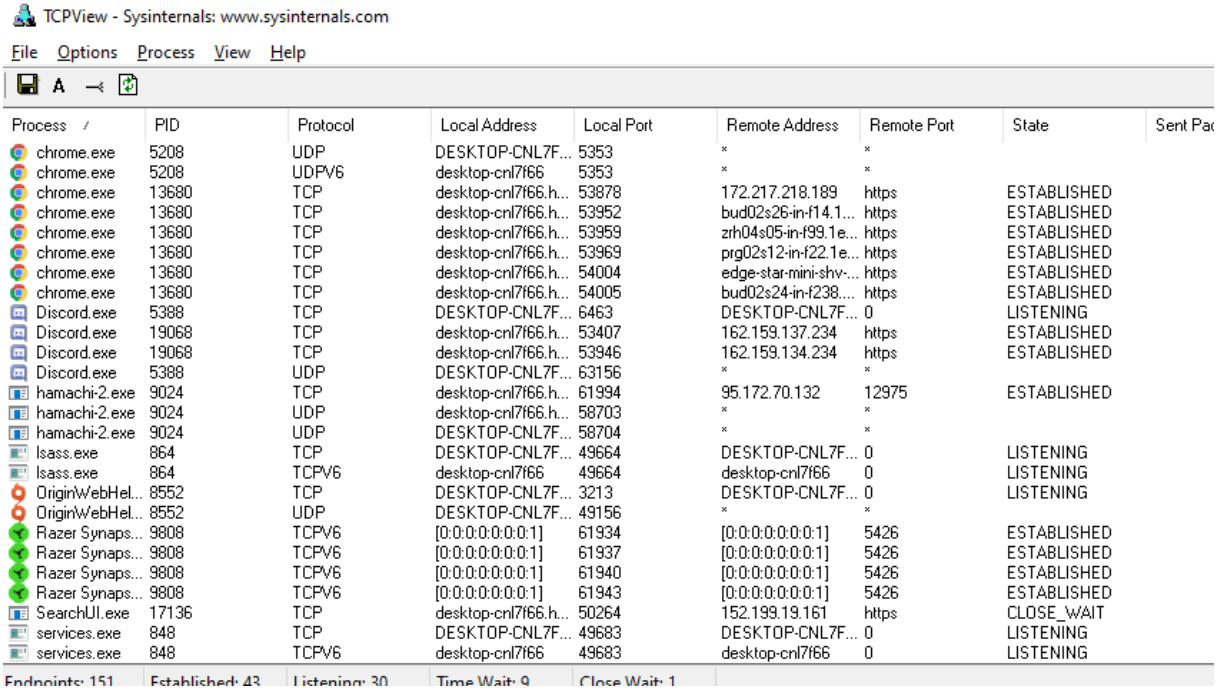


Egy futó alkalmazásra jobb gombbal kattintva majd a properties menüpontot kiválasztva Részletes információt kapunkhatunk róla. Ilyenek például: a verziószám, a program indulási helye, adott user azonosító, aki használja és a futtatás kezdetének időpontja.A Performance fülön keresztül pedig további információkhoz juthatunk a processzor, a virtuális, illetve fizikai memória adatairól, valamint a I/O műveletekről.





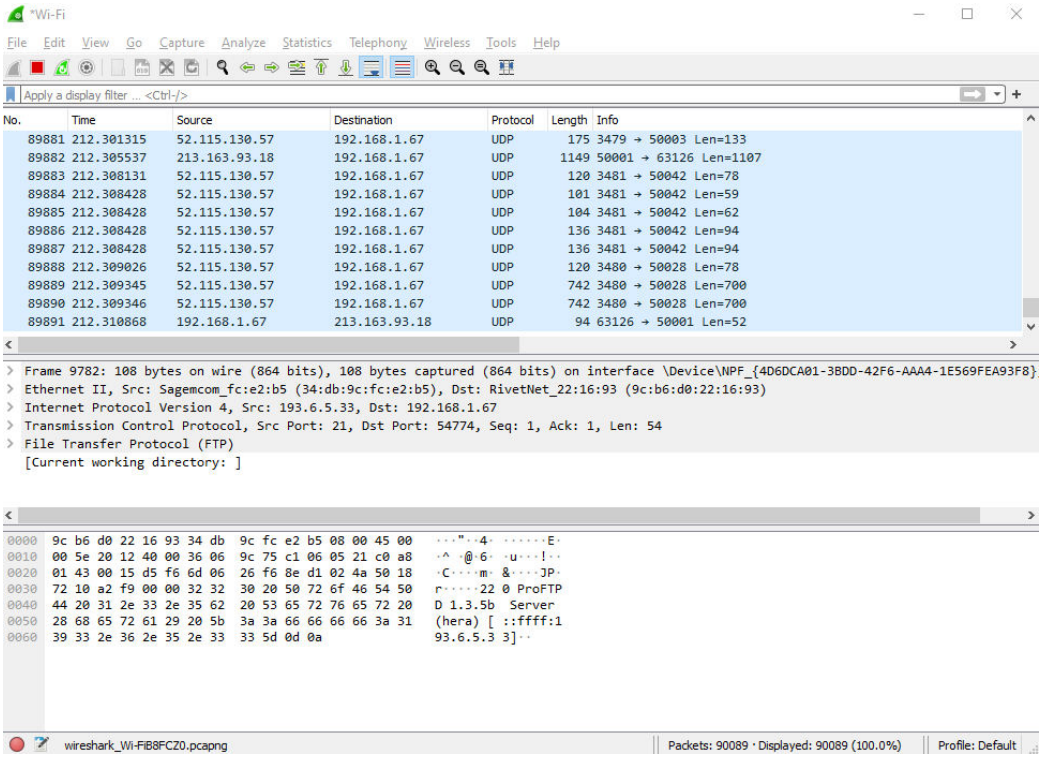
A harmadik TcpView melyel az éppen futó alkalmazások hálózati használati tulajdonságát tudom elemezni. A state oszlopban a státusz tulajdonság szerepel mely azt jelzi, hogy a program vár a kapcsolódásra 'Listening' vagy pedig már kapcsolódott 'Established'.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Pac
chrome.exe	5208	UDP	DESKTOP-CNL7F...	5353	*	*		
chrome.exe	5208	UDPV6	desktop-cnl7f66	5353	*	*		
chrome.exe	13680	TCP	desktop-cnl7f66.h...	53878	172.217.218.189	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66.h...	53952	bud02s26-in-f14.1...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66.h...	53959	zrh04s05-in-f99.1e...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66.h...	53969	prg02s12-in-f22.1e...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66.h...	54004	edge-star-mini-shv-...	https	ESTABLISHED	
chrome.exe	13680	TCP	desktop-cnl7f66.h...	54005	bud02s24-in-f238....	https	ESTABLISHED	
Discord.exe	5388	TCP	DESKTOP-CNL7F...	6463	DESKTOP-CNL7F...	0	LISTENING	
Discord.exe	19068	TCP	desktop-cnl7f66.h...	53407	162.159.137.234	https	ESTABLISHED	
Discord.exe	19068	TCP	desktop-cnl7f66.h...	53946	162.159.134.234	https	ESTABLISHED	
Discord.exe	5388	UDP	DESKTOP-CNL7F...	63156	*	*		
hamachi-2.exe	9024	TCP	desktop-cnl7f66.h...	61994	95.172.70.132	12975	ESTABLISHED	
hamachi-2.exe	9024	UDP	desktop-cnl7f66.h...	58703	*	*		
hamachi-2.exe	9024	UDP	DESKTOP-CNL7F...	58704	*	*		
lsass.exe	864	TCP	DESKTOP-CNL7F...	49664	DESKTOP-CNL7F...	0	LISTENING	
lsass.exe	864	TCPV6	desktop-cnl7f66	49664	desktop-cnl7f66	0	LISTENING	
OriginWebHel...	8552	TCP	DESKTOP-CNL7F...	3213	DESKTOP-CNL7F...	0	LISTENING	
OriginWebHel...	8552	UDP	DESKTOP-CNL7F...	49156	*	*		
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:0:1]	61934	[0:0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:0:1]	61937	[0:0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:0:1]	61940	[0:0:0:0:0:0:0:1]	5426	ESTABLISHED	
Razer Synaps...	9808	TCPV6	[0:0:0:0:0:0:0:1]	61943	[0:0:0:0:0:0:0:1]	5426	ESTABLISHED	
SearchUI.exe	17136	TCP	desktop-cnl7f66.h...	50264	152.199.19.161	https	CLOSE_WAIT	
services.exe	848	TCP	DESKTOP-CNL7F...	49683	DESKTOP-CNL7F...	0	LISTENING	
services.exe	848	TCPV6	desktop-cnl7f66	49683	desktop-cnl7f66	0	LISTENING	

Endpoints: 151 Established: 43 Listening: 30 Time Wait: 9 Close Wait: 1

Végül már csak a wireShark maradt kipróbálásra.



A leírtak szerint a Commanderrel bejelentkeztem a Miskolci egyetem ftp-szerverére és ki capture-öltem a bejelentkezési információkat.